Comportement WSA sur la découverte de MTU de chemin avec l'utilisation du WCCP

Contenu

Introduction

Ce document décrit un problème rencontré où le routeur relâche des paquets quand votre configuration inclut le Web Cache Communication Protocol (WCCP) et détection de Maximum Transmission Unit de chemin (MTU), et elle fournit une solution au problème.

Informations générales

Pré-phase

Une fois regardées séparément, beaucoup de caractéristiques sont excellentes pour traiter un problème spécifique. Parfois cependant, si vous combinez deux ou trois techniques, il produit un certain comportement maladroit et vous devez introduire une caractéristique ou un contournement différente afin de le faire fonctionner correctement. Par exemple, le spanning-tree d'utilisation et le Protocole OSPF (Open Shortest Path First) et posent 2 (L2) que la convergence prend plus long (20s) qu'OSPF (1s si l'intervalle mort minimum est utilisé), mais remplacent le spanning-tree par le plusieurs spanning-tree (MST) et elle fonctionne correctement de nouveau.

On a observé le même comportement d'Interopérabilité entre le WCCP et la découverte de MTU de chemin ; beaucoup pensent que c'est le problème d'en-tête d'Encapsulation de routage générique (GRE). Cependant, ce document explique la vraie cause.

Comment la découverte de MTU de chemin et le WCCP fonctionnent séparément

Découverte de MTU de chemin

Chaque ligne a sa limite sur la façon dont grand un paquet peut être. Si vous envoyez un plus grand paquet qu'est pris en charge, alors il est lâché. Un des rôles des périphériques L3 (Routeurs) sur le chemin est de salut et la côtelette de grands paquets d'une des lignes aux autres afin de s'assurer que la transmission de bout en bout est transparente aux capacités de chaque ligne.

Parfois cependant, des hôtes d'extrémité sont configurés de telle manière que leurs paquets ne puissent pas être coupés (par exemple, des fichiers cryptés, des communications voix). Ces informations sont communiquées par l'intermédiaire du Don't Fragment (DF) mordu à l'intérieur de l'en-tête IP. Les Routeurs relâchent des paquets comme ces derniers, mais les essais de routeur pour faire rapport à l'hôte d'extrémité par l'intermédiaire du message de Protocole ICMP (Internet Control Message Protocol) (le type 3-Destination inaccessible, codent 4 - fragmentation requise, mais bit DF réglé). De cette façon, l'hôte sait pour envoyer de plus petits paquets à l'avenir.

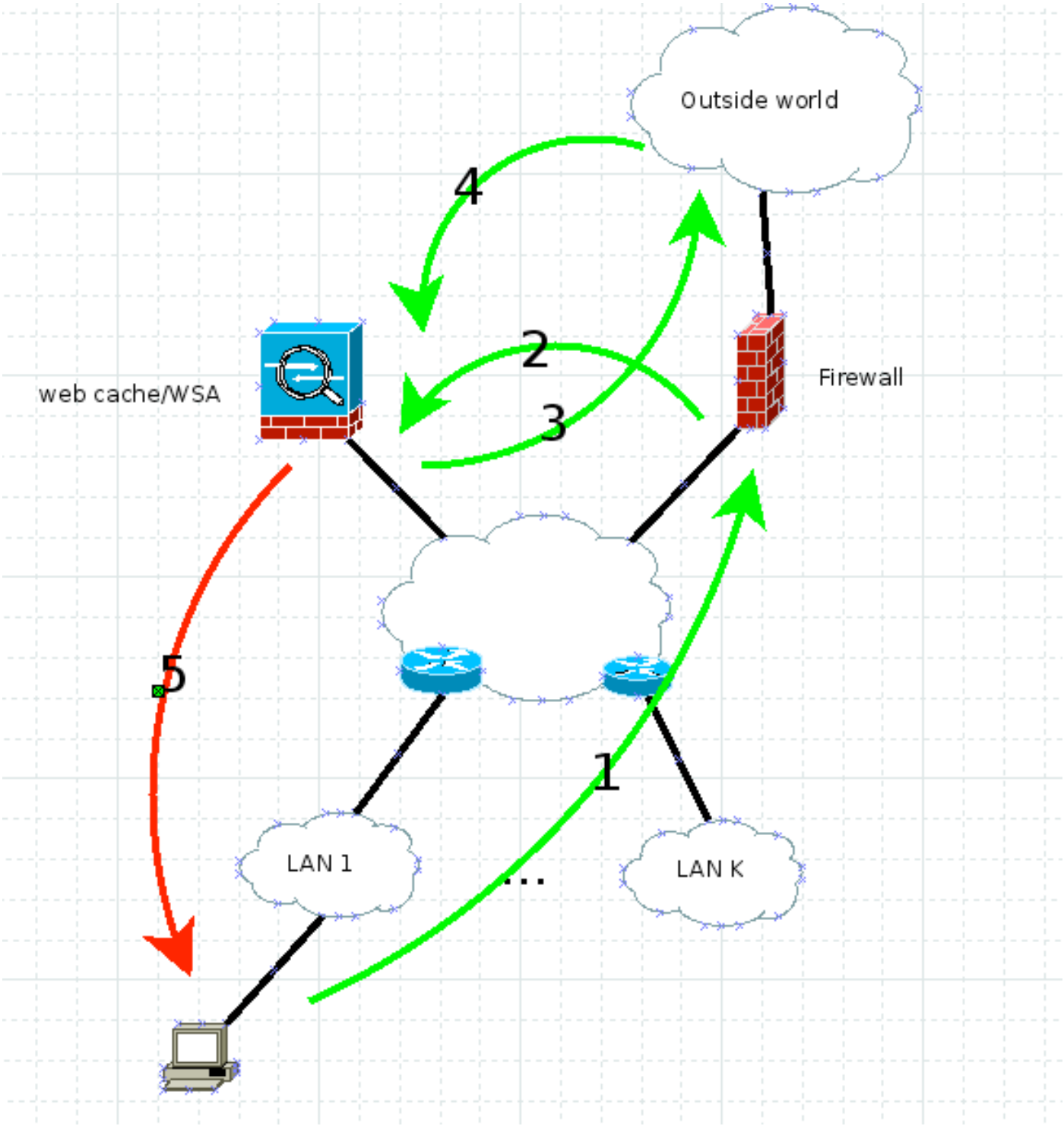
C'est le coeur de la découverte de MTU de chemin. Vous pouvez envoyer de grands paquets avec le bit DF réglé afin de voir s'ils le font vers l'extrémité ou si vous recevez un rapport ICMP comme décrit précédemment. Une fois que vous déterminez la longueur de paquet réalisable maximum, utilisez-la pour toute autre transmission. Référez-vous au pour en savoir plus RFC 1191.

L'appliance de sécurité Web (WSA) utilise la découverte de MTU de chemin par défaut. Ainsi, tous ses paquets générés ont le bit DF réglé par la configuration par défaut.

WCCP

Si vous devez imposer la Sécurité dans votre réseau au trafic web sans d'autres la connaissance, vous exécutez leur trafic par l'intermédiaire d'un proxy qui n'est pas visible. Le WCCP est le protocole qui est utilisé pour communiquer entre le périphérique qui intercepte (routeur/Pare-feu) et le moteur de cache Web/proxy, qui est WSA dans ce cas.

Ce diagramme montre comment la circulation dans ce scénario :



Cela fonctionne comme ceci :

1. Le client envoie le HTTP OBTIENNENT avec la source IP, son adresse IP (adresse IP de client), et l'adresse IP de serveur cible.

2. Le Pare-feu ou le routeur intercepte le HTTP OBTIENNENT et en avant il par l'intermédiaire de WCCP GRE ou L2 pur au Web cache/WSA. La source est toujours l'adresse IP de client et la destination est toujours l'adresse IP de web server.

3. Le WSA examine la demande et, s'il est légitime, la reflète vers le web server. Ici l'adresse IP de destination est l'adresse IP de web server et l'adresse IP source pourrait être les WSA ou le client, basés en fonction si vous avez activé la mystification d'adresse IP de client. Pour cet exemple, il n'importe pas parce que le trafic de retour dans des les deux cas doit frapper

le WSA.

4. Le trafic de retour est examiné au WSA.

5. Le WSA envoie la réponse au client avec l'adresse IP source, TOUJOURS l'adresse IP de web server (ainsi le client n'obtient pas méfiant), et l'adresse IP de client de destiantion.

Problème

Que se produit si un des Routeurs du diagramme doit fragmenter le trafic ? Le WSA met le bit DF sur le paquet le numéro 5, mais il doit être fragmenté. Le routeur le relâche et dit à l'expéditeur que la fragmentation est nécessaire mais le bit DF est placé (code de type ICMP 3 4). Après tout, RFC 1191 doit fonctionner maintenant et l'expéditeur doit diminuer sa longueur de paquet.

Avec le WCCP, l'adresse IP source est l'adresse IP de web server, ainsi cet ICMP ne va jamais au WSA ; en revanche, il essaye d'aller au vrai web server (souvenez-vous, ce routeur sur le bas ne se rend pas compte du WCCP). C'est comment le WCCP et la découverte de MTU de chemin cassent ensemble parfois votre conception de réseaux.

Solution

Il y a quatre manières de résoudre ce problème :

- Découvrez le vrai MTU et puis employez l'**etherconfig** sur le WSA pour diminuer le MTU de l'interface. Souvenez-vous que l'en-tête de TCP est 60, l'IP est 20, et quand vous utilisez l'ICMP, qui ajoute 8 octets à l'en-tête IP.

- Découverte de MTU de chemin de débronchement (commande CLI WSA de **pathmtudiscovery**). Ceci a comme conséquence le TCP MSS de 536, qui pourraient poser un problème de performances.

- Changez le réseau tellement là n'est aucune fragmentation L3 entre le WSA et les clients.

- Utilisez le **TCP d'IP mss-ajustent** nombres calculés) la commande **1360** (ou autres sur chaque routeur de Cisco sur le chemin sur les interfaces appropriées.

Notes supplémentaires

Tandis que ce problème était à l'étude, on l'a découvert que si vous placez le proxy explicitement dans le client pendant quelques minutes et le retirez alors, la question est résolue pour les quatre à cinq heures suivantes. C'est dû au fait que, en mode explicite, mécanisme de découverte de MTU de chemin entre le WSA et les travaux de client. Une fois que le WSA découvre le MTU de chemin, il l'enregistre avec le TCP MSS découvert sur la table interne pour la référence. Apparemment cette table est régénérée toutes les quatre à cinq heures, qui rend la solution pour ne pas fonctionner de nouveau après tellement temps.